In The Claims

1. (Original) A method of authenticating, using an authentication server, the use of an authentication device over a communication network via an intermediate communication device, comprising:

receiving an authentication datagram by said intermediate device;

protecting said datagram by said intermediate device, by at least one of changing, adding to, encrypting and signing of said datagram; and

forwarding said datagram to said authentication server for authentication.

2. (Currently Amended) A method according to claim 1, wherein said intermediate device comprises a vendor ~~WWW~~World Wide Web site.

3. (Original) A method according to claim 2, wherein protecting comprises adding a signature associated with said vendor to said datagram.

4. (Original) A method according to claim 2, wherein protecting comprises encrypting said datagram.

5. (Previously Presented) A method according to claim 1, wherein said intermediate device comprises a user computing device.

6. (Original) A method according to claim 5, wherein said computing device adds a time stamp to said datagram.

7. (Original) A method according to claim 5, wherein said computing device adds a vendor-associated information item to said datagram.

8. (Original) A method according to claim 5, wherein said computing device encrypts said datagram.

9. (Original) A method according to claim 8, wherein said encryption uses a one time code.

10. (Previously Presented) A method according to claim 8, wherein said one time code is provided by a vendor for a particular session with said user.

11. (Original) A method according to claim 5, wherein said user computing device uses an embedded software component for said protecting.

12. (Original) A method according to claim 11, wherein said embedded software comprises an ActiveX component.

13. (Original) A method according to claim 11, wherein said component is cached on said user device.

14. (Original) A method according to claim 11, wherein said component requires a property value provided by a vendor to operate.

15. (Original) A method according to claim 1, wherein communication between said intermediate device and said server uses a secure connection.

16. (Original) A method according to claim 1, wherein different communication paths are used for said authentication and for transaction details from said user.

17. (Original) A method according to claim 1, wherein different communication paths are used for said authentication and for transaction details from a vendor to said authentication server.

18. (Currently Amended) A method of authentication of an authentication datagram by a remote authentication server, comprising:

sending an encrypted ~~datagarm~~datagram by secure computer communication from a vendor software to said remote authenticator;

_____receiving said encrypted datagram by said remote authenticator;_

comparing said datagram or a hash thereof to a hash table at said server; ~~and~~

4

generating a binary validation answer by said server without an associated explanation; and

      outputting said binary validation answer.

19. (Currently Amended) A method of authentication of an authentication datagram by a remote authentication server, comprising:

      sending an encrypted datagram by computer communication from an authentication device to said remote authentication server;

      receiving said encrypted datagram by said remote authentication server;

      searching, at said server, for a hash value matching said datagram or a hash thereof;

~~and~~

      generating a validation answer by said remote authentication server, responsive to said search,

      wherein, said datagram includes a secret code and wherein said secret code exists only on said authentication device; and

      outputting said validation answer.

20. (Original) A method according to claim 19, wherein said authentication device includes a plurality of secret codes that are generated to appear unrelated.

21. (Currently Amended) A method of generating a code set for ~~an~~a remote authentication device, comprising:

      providing a code generating software;

      providing at least one seed code for said software;

      generating said code set using said software and said seed;

      destroying said seed immediately after generating said code set;

      forwarding said code set to said authentication device; and

      storing said code set or an indication thereof on ~~an~~said remote authentication device.

22. (Original) A method according to claim 21, comprising generating hash values for said code set.

23. (Original) A method according to claim 22, comprising generating a second set of hash values for said code set, using a different hash function for said second set.

24. (Currently Amended) A method of communication between a vendor and a user using an authentication device, comprising:

      generating a one time code for the user for a session;

      receiving an authentication datagram from said user; and

      ~~passing on~~forwarding said datagram ~~for verification by~~to a remote authentication server for authentication if at least an indication of said one time code that matches said user is provided with said datagram.

25. (Original) A method according to claim 24, comprising signing said datagram using said one time code by said user.

26. (Currently Amended) A method of remote validation, comprising:

      receiving an authentication datagram by an authentication server from a remote authentication device;

      matching said datagram or a hash of said datagram to a table;

      calculating a counter value from a matching position in said table; and

      ~~validating~~if said authentication datagram is valid, ~~based on an increase in~~increasing said counter over a previous counter, ~~being~~within a certain limit; and

      outputting a validation signal.

27. (Original) A method according to claim 26, comprising:

      failing said authentication based on said increase being too large; and

      allowing a subsequent authentication based on a further increase of said subsequent validation being below a second threshold.

28. (Original) A method according to claim 27, wherein said thresholds are the same.

29. (Original) A method according to claim 27, wherein said second threshold is smaller than said certain threshold.

30. (Previously Presented) A method according to claim 26, wherein said counter comprises an ordinal position in said table that is not apparently related to a series of generated random numbers.

31. (Currently Amended) A method of detecting a transmission of an acoustic multitone ~~FSK~~Frequency Shift Key (FSK) signal comprising:

receiving an acoustic signal;

converting the signal into a Hilbert-transform representation of the signal;

correlating said converted signal with at least one reference signal representing at least one expected frequency in said FSK signal;

integrating said correlation over an interval; ~~and~~

~~determining~~ if a signal is present, based on a thresholding of a result of said integrating, generating a validation signal; and

outputting said validation signal.

32. (Original) A method according to claim 31, comprising further determining if a detected signal has a frequency within a certain frequency range.

33. (Previously Presented) A method according to claim 31, comprising further determining if a detected signal has a signal to noise ratio within a certain signal to noise ratio range.

34. (Original) A method according to claim 31, comprising resampling said signal after said determining.

35. (Original) A method according to claim 31, wherein said threshold is noise dependent of the received signal.

36. (Original) A method according to claim 31, comprising calculating said interval based on a hardware characteristic of a producer of said acoustic signal.